Operations Dialogue

Brian Snodgrass

CIO Council Meeting
March 9, 2011

IT INFRASTRUCTURE PARTNERSHIP

VITA   **NORTHROP GRUMMAN**

2011 hardware request forms include all identified 2011 eligible devices

- Provided to agencies by mid-February

- Refresh schedules based on eligible refresh date and geographic locations

- Active and not-billed assets reported via:
  - ➤ Asset management survey
  - ➤ Asset management billing data
  - ➤ PARS, Altiris, Active Directory, CISCO, ePO/Security

Agencies to…

- Validate end user and address information

- Select hardware type desired for replacement

- Indicate devices for IMAC, billing dispute

- Return form to AOM with any agency blackout dates

- Approve schedule (or revise as required); return to PC refresh team

PC refresh team to…

- Schedule devices for refresh; provide agency a schedule for approval

- Order/ship standard devices

- Advise agency when to submit eVA request for incremental items

- Begin refreshing devices

PC Refresh – 2011 Top 12 Agencies

Agency	Months												TOTAL	MSR Status
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec		
VDH	94	62	163	265	131	100	69	70	125	391	253	73	**1796**	MSR expected by 3/11
DOC	4	2	27	17	210	146	226	399	428	136	19	52	**1666**	Initial MSR with 500+ devices provided
DMV	3	8	28	131	10	19	978	55	1	7	7		**1247**	Thin to thick client and others in progress
VEC		106	9		14		19	5	1	113	76	630	**973**	Awaiting completion of MSR
DJJ	2	14	69	124	49	23	23	26	36	13	16	9	**404**	Awaiting completion of MSR
VDOT	11	34	21	21	27	9	6	33	30	23	41	72	**328**	Awaiting completion of MSR
DGIF		1	32	180	3			7	20				**243**	Agency reviewing inventory
ABC							9	78	1	98		1	**187**	Awaiting completion of MSR
DSS	4		2	5	4	22	13	36	44	9	16	15	**170**	Awaiting completion of MSR
VITA			3	3	12	18	2	24	18	59	4	1	**144**	Agency reviewing inventory
TAX			30					5	17		6	32	**90**	TAX to provide MSR by 3/15
DCE		1	1	4	50	2	2	7	2	3	1	4	**77**	DCE to provide MSR by 3/10

Server Refresh Methodology

▶ There is no defined interval refresh policy for servers; we use situational refresh only.

▶ Situational refresh drivers are events or conditions that impact, or reasonably could be expected to impact, service level agreement (SLA) compliance. These will be investigated and the root cause analysis (RCA) results may justify refresh.

Server Refresh Methodology

▸ Representative events or conditions include the following:

- End of support (EOS) notice for an operating system
- Repeated failures of the same component within a specific system
- Original equipment manufacturer (OEM) stated end of life (EOL) for server family
- Component manufacturer issues recall notice
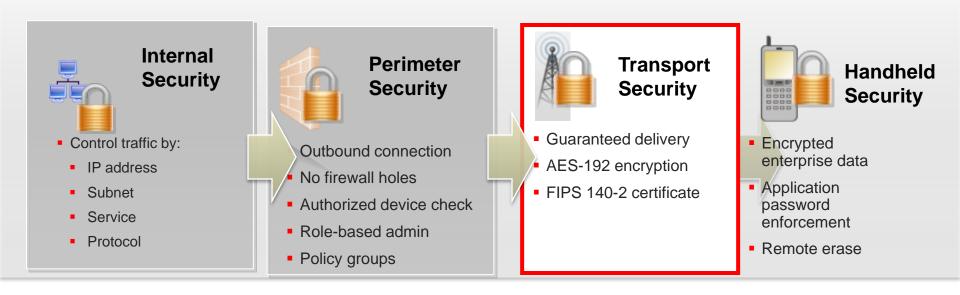- Technical or standards currency

Server Refresh Methodology

▸ The following events and conditions, commonly perceived to be refresh triggers, do not by themselves, justify refresh:

  – Service platform age as a sole factor

  – Workload growth

  – Issues that can be remediated through repairing, replacing or augmenting server components

▸ Open discussion

Smart Devices - Solution Attributes

■ **Separate:** "Quarantine" enterprise data on devices—
without interfering with personal information and applications.

■ **Secure:** Ensure security at each level of data delivery—
internal, perimeter, transport and at the handheld device.

■ **Managed:** Manage the whole device or just the business applications and data
consistently and in accordance with COV policies and standards.

Internal Security

- Control traffic by:
  - IP address
  - Subnet
  - Service
  - Protocol

Perimeter Security

- Outbound connection
- No firewall holes
- Authorized device check
- Role-based admin
- Policy groups

Transport Security

- Guaranteed delivery
- AES-192 encryption
- FIPS 140-2 certificate

Handheld Security

- Encrypted enterprise data
- Application password enforcement
- Remote erase

Smart Devices - Phone Support

Personal Data

Devices remain personal, untouched by enterprise

- Justifies shared employee expense

Freely access your own stuff

- Applications
- Pictures
- Videos

Enterprise Data

Enterprise data lockdown

- Data encryption
- Password policies
- Remote wipe
- Secure data at rest

Access corporate apps

- E-mail, attachments
- Intranets
- Document repositories

Employees are more likely to accept an "enterprise-grade" mobile security policy when enterprise control is "contained" and does not impact personal experience, apps or data

▸ Deploy UCaaS voice over Internet protocol (VoIP) phones as the Commonwealth standard

    – Northrop Grumman will work with agencies to identify current telco costs vs. UCaaS voice service costs

    – UCaaS provides agency opportunity to expand into video teleconferencing

▸ Move away from PBX and premise phone systems

– Will use VoIP-to-analog adapters for locations that cannot easily support CAT5 wiring

– Developing pricing structure for agencies to use one-time funds to lower monthly UCaaS service charges

Voice Strategy

▸ Deploy key systems as needed at smaller Commonwealth locations

– Where UCaaS voice service costs may exceed current telco costs (large number of handsets and few telco lines), deploy key systems

– Working with Cisco to deploy common key system type to leverage common phone handset, hardware and software support model

Questions